МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

Микола АФАНАСЬЄВ

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший(бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	**базова**
Мова викладання, навчання таоцінювання	**українська**

Завідувач кафедри
кібербезпеки та інформаційних технологій *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 2 від 31.08.2020 р.

Розробник(-и):
Корольов Р.В., к.т.н., доцент кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальноїдисципліни

Природні канали витоку інформації утворюються спонтанно, в силу специфічних обставин, що склалися на об'єкті захисту. Що стосується штучних каналів витоку інформації, то вони створюються навмисно із застосуванням активних методів і способів отримання інформації. Активні способи припускають навмисне створення технічних каналів витоку інформації з використанням спеціальних технічних засобів. До них можна віднести незаконне підключення до каналів, проводам і лініям зв'язку, високочастотне нав'язування і опромінення, установка в технічних засобах і приміщеннях відеокамер, мікрофонів і телефонних закладних пристроїв, а також несанкціонований доступ до інформації, що обробляється в автоматизованих системах тощо.

Тому особливу роль і місце в діяльності по захисту інформації займають заходи щодо створення комплексного захисту, що враховують загрози національній і міжнародній безпеці і стабільності, в тому числі суспільству, особистості, державі, демократичних цінностей і суспільних інститутів, суверенітету, економіці, фінансовим установам, розвитку держави.

Метою викладання навчальної дисципліни є навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

Результатами вивчення даної дисципліни є придбання навичок з захисту інформації в інформаційно-комунікаційних системах від витоку інформації по технічними каналами зв'язку, порядку проведення обстеження середовищ функціонування інформаційно телекомунікаційних систем.

Характеристика навчальної дисципліни

Курс	**3**
Семестр	**5**
Кількість кредитів ECTS	**5**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Вища математика	**Основи стегонаграфічного зазисту**
Математичні основи криптології	
ІС і Інтернет-технології	

Компетентності та результати навчання задисципліною

Компетентності	Результати навчання
КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

Компетентності	Результати навчання
	РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

Компетентності	Результати навчання
	РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Програма навчальної дисципліни

Змістовий модуль 1.Нормативно-правові аспекти побудови КСЗІ. Захист інформації від технічних каналів витоку.

Тема 1. *Нормативно-правове забезпечення в сфері інформаційної безпеки.*

Тема 2. *Захист інформації в інформаційно-комунікаційних системах від витоку технічними каналами.*

Тема 3. *Радіоканали витоку інформації.*

Тема 4. *Акустичні канали витоку інформації та методи захисту.*

Тема 5. *Побічні електромагнітні випромінювання (ПЕМВ) засобів обчислювальної техніки (ЗОТ).*

Тема 6. *Загрози інформації в сучасних ІКС.*

Тема 7. *Канали витоку при експлуатації ЕОМ.*

Змістовий модуль 2. Створення КСЗІ в інформаційно-телекомунікаційних системах

Тема 8. *Формування загальних вимог до КСЗІ в ІКС.*

Тема 9.*Етапи побудови КСЗІ.*

Перелік практичних (семінарських) / лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, дискусії, презентації, бесіди, індивідуальні та групові проєкти.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- вміння критично осмислювати, вибирати та використовувати необхідний

науковий, методичний і аналітичний інструментарій для управління в непередбачуваних умовах;

- вміти приймати, обґрунтовувати та забезпечувати реалізацію управлінських рішень в непередбачуваних умовах, враховуючи вимоги чинного законодавства, етичні міркування та соціальну відповідальність;
- вміння забезпечувати особистий професійний розвиток та планувати власний часу.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі накопичених балів за виконані поточні та контрольні завдання з лекційних та лабораторних занять, що відображає розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатність творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Практичні (семінарські, лабораторні) заняття: максимальна кількість балів становить 88, а мінімальна – 44.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку їх захисту й виконання контрольних робіт з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться за накопиченими балами.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час заліку, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1.	***Аудиторна робота***			
	Лекція	Лекція №1. Нормативно-правове забезпечення в сфері інформаційної безпеки.	Робота на лекції	2
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція №2. Захист інформації в інформаційно-комунікаційних системах від витоку технічними каналами.	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 1. Встановлення Kali Linux на комп'ютер або віртуальну машину(флеш носій або зовнішній диск).	Захист лабораторної роботи	12
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція №3. Радіоканали витоку інформації.		1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 4.	***Аудиторна робота***			
	Лекція	Лекція №4. Акустичні канали витоку інформації та методи захисту.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 2. Дослідження стійкості точок доступу бездротової мережі Wi-Fi.	Захист лабораторної роботи	12
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 5.	***Аудиторна робота***			
	Лекція	Лекція №5. Побічні електромагнітні випромінювання (ПЕМВ) засобів обчислювальної	Робота на лекції	1

		техніки (ЗОТ).		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 6.	***Аудиторна робота***			
	Лекція	Лекція №6. Загрози інформації в сучасних ІКС.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 3. Використання утиліт Kali Linux для створення словників.	Захист лабораторної роботи	12
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 7.	***Аудиторна робота***			
	Лекція	Лекція №7. Канали витоку при експлуатації ЕОМ.	Робота на лекції	1
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 8.	***Аудиторна робота***			
	Лекція	Лекція №8. Формування загальних вимог до КСЗІ в ІКС.	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота 4. Використання сканера безпеки Nmap та Zmap на Kali Linux.	Захист лабораторної роботи	12
			Контрольна робота	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 9.	***Аудиторна робота***			
	Лекція	Лекція №9. Етапи побудови КСЗІ.	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 5. Використання інструментарію соціальної інженерії використовуємих в Kali Linux.	Захист лабораторної роботи	12
			Контрольна робота	3
	Самостійна робота			
	Питання та завдання	Пошук, підбір та огляд		

	до самостійного опрацювання	літературних джерел за заданою тематикою		
Тема 10.	***Аудиторна робота***			
	Лабораторне заняття	Лабораторна робота 6. Дослідження стійкості парольного захисту за допомогою спеціального програмного забезпечення.	Захист лабораторної роботи	12
			Контрольна робота	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Рекомендована література

Основна

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994)
2. Закон України “Про захист персональних даних” (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України “Про національну безпеку (2018)
5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації вкомп'ютерних системах від несанкціонованого доступу.
16. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації віднесанкціонованого доступу.
17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексноїсистеми захисту інформації в інформаційно-телекомунікаційній системі.
18. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічногозавдання на створення комплексної системи захисту інформації в АС.
19. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація зобмеженим доступом, що становить державну таємницю.
20. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e

Додаткова

21.ISO/IEC 27001. "Информационные технологии. Методы обеспечениябезопасности. Системы управления информационной безопасностью.

22. ISO/IEC 27002. "Информационные технологии. Методы обеспечениябезопасности. Практические правила управления информационнойбезопасностью."

23. ISO/IEC 27005. "Информационные технологии. Методы обеспечениябезопасности. Управление рисками информационной безопасности

Інформаційні ресурси

24. http://bezopasnost.biz

25. http://dstszi.gov.ua

26. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “ Комплексні системи захисту інформації” https://pns.hneu.edu.ua/course/view.php?id=4940